United Nations A/70/174

General Assembly

Distr.: General
22 July 2015

Original: English

**Seventieth session**
Item 93 of the provisional agenda*
**Developments in the field of information and telecommunications in the context of international security**

# Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

## Note by the Secretary-General

The Secretary-General has the honour to transmit herewith the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. The Group was established pursuant to paragraph 4 of General Assembly resolution 68/243.

* A/70/150.

15-12404 (E) 180815

Please recycle

# Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

*Summary*

Information and communications technologies (ICTs) provide immense opportunities and continue to grow in importance for the international community. However, there are disturbing trends that create risks to international peace and security. Effective cooperation among States is essential to reduce those risks.

The 2015 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security examined existing and potential threats arising from the use of ICTs by States and considered actions to address them, including norms, rules, principles and confidence-building measures. In addition, the Group examined how international law applies to the use of ICTs by States. Building on the work of previous Groups, the present Group made important progress in those areas.

The present report significantly expands the discussion of norms. The Group recommended that States cooperate to prevent harmful ICT practices and should not knowingly allow their territory to be used for internationally wrongful acts using ICT. It called for the increased exchange of information and assistance to prosecute terrorist and criminal use of ICTs. In doing so, the Group emphasized that States should guarantee full respect for human rights, including privacy and freedom of expression.

One important recommendation was that a State should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure. States should also take appropriate measures to protect their critical infrastructure from ICT threats. States should not harm the information systems of the authorized emergency response teams of another State or use those teams to engage in malicious international activity. States should encourage the responsible reporting of ICT vulnerabilities and take reasonable steps to ensure the integrity of the supply chain and prevent the proliferation of malicious ICT tools, techniques or harmful hidden functions.

Confidence-building measures increase cooperation and transparency and reduce the risk of conflict. The Group identified a number of voluntary confidence-building measures to increase transparency and suggested that States consider additional ones to strengthen cooperation. The Group called for regular dialogue with broad participation under the auspices of the United Nations and through bilateral, regional and multilateral forums. While States have a primary responsibility to maintain a secure and peaceful ICT environment, international cooperation would benefit from the appropriate participation of the private sector, academia and civil society.

Capacity-building is essential for cooperation and confidence-building. The 2013 report of the Group (see A/68/98) called for the international community to assist in improving the security of critical ICT infrastructure, help to develop technical skills and advise on appropriate legislation, strategies and regulation. The present Group reiterated those conclusions and emphasized that all States can learn from each other about threats and effective responses to them.

The Group emphasized the importance of international law, the Charter of the United Nations and the principle of sovereignty as the basis for increased security in the use of ICTs by States. While recognizing the need for further study, the Group noted the inherent right of States to take measures consistent with international law and as recognized in the Charter. The Group also noted the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction.

In its thinking on future work, the Group proposed that the General Assembly consider convening a new Group of Governmental Experts in 2016.

The Group asks Member States to actively consider their recommendations and assess how they might be taken up for further development and implementation.

## Contents


| | | *Page* |
|---|---|---|
| | Foreword by the Secretary-General | 4 |
| | Letter of transmittal | 5 |
| I. | Introduction | 6 |
| II. | Existing and emerging threats | 6 |
| III. | Norms, rules and principles for the responsible behaviour of States | 7 |
| IV. | Confidence-building measures | 9 |
| V. | International cooperation and assistance in ICT security and capacity-building | 10 |
| VI. | How international law applies to the use of ICTs | 12 |
| VII. | Conclusions and recommendations for future work | 13 |
| Annex | | 15 |

## Foreword by the Secretary-General

Few technologies have been as powerful as information and communications technologies (ICTs) in reshaping economies, societies and international relations. Cyberspace touches every aspect of our lives. The benefits are enormous, but these do not come without risk. Making cyberspace stable and secure can be achieved only through international cooperation, and the foundation of this cooperation must be international law and the principles of the Charter of the United Nations.

The present report contains recommendations developed by governmental experts from 20 States to address existing and emerging threats from uses of ICTs, by States and non-State actors alike, that may jeopardize international peace and security. The experts have built on consensus reports issued in 2010 and 2013, and offer ideas on norm-setting, confidence-building, capacity-building and the application of international law.

Among the complex issues that have emerged is the growing malicious use of ICTs by extremists, terrorists and organized criminal groups. The present report provides suggestions that can help to address this worrisome trend and contribute to the formulation of my forthcoming plan of action on preventing violent extremism.

All States have a stake in making cyberspace more secure. Our efforts in this realm must uphold the global commitment to foster an open, safe and peaceful Internet. In that spirit, I commend the present report to the General Assembly and to a wide global audience as a crucial contribution to the vital effort to secure the ICT environment.

## Letter of transmittal

26 June 2015

I have the honour to submit herewith the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. The Group was established in 2014 pursuant to paragraph 4 of General Assembly resolution 68/243 on developments in the field of information and telecommunications in the context of international security. As Chair of the Group, I am pleased to inform you that consensus was reached on the report.

In its resolution, the General Assembly requested that a group of governmental experts be established in 2014, on the basis of equitable geographical distribution, to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behaviour of States and confidence-building measures, the issues of the use of information and communications technologies in conflicts and how international law applies to the use of information and communications technologies by States, as well as the concepts aimed at strengthening the security of global information and telecommunications systems. The Group was also asked to take into account the assessments and recommendations of a previous Group (see A/68/98). The Secretary-General was requested to submit a report on the results of the study to the Assembly at its seventieth session.

In accordance with the terms of the resolution, experts were appointed from 20 States: Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, the Republic of Korea, the Russian Federation, Spain, the United Kingdom of Great Britain and Northern Ireland and the United States of America. The list of experts is contained in the annex.

The Group had a comprehensive, in-depth exchange of views on developments in the field of information and telecommunications in the context of international security. It met in four sessions: the first from 21 to 25 July 2014 at United Nations Headquarters, the second from 12 to 16 January 2014 in Geneva and the third from 13 to 17 April 2015 and the fourth from 22 to 26 June 2015, both at United Nations Headquarters.

The Group would like to thank the experts who served as facilitators in the discussions on the draft report: Florence Mangin (France), Katherine Getao (Kenya), Ausaf Ali (Pakistan), Ricardo Mor (Spain) and Olivia Preston (United Kingdom).

The Group wishes to express its appreciation for the contribution of the United Nations Institute for Disarmament Research, which served as a consultant to the Group and was represented by James Lewis and Kerstin Vignard. The Group also wishes to express its appreciation to Ewen Buchanan of the United Nations Office for Disarmament Affairs, who served as Secretary of the Group, and to other Secretariat officials who assisted the Group.

(*Signed*) Carlos Luís Dantas Coutinho **Perez**
Chair of the Group

# I. Introduction

1. Pursuant to General Assembly resolution 68/243 on developments in the field of information and telecommunications in the context of international security, the Secretary-General, on the basis of equitable geographical distribution, established a group of governmental experts to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behaviour of States and confidence-building measures, the issues of the use of information and communications technologies (ICTs) in conflicts and how international law applies to the use of ICTs by States, as well as relevant international concepts aimed at strengthening the security of global information and telecommunications systems.

2. An open, secure, stable, accessible and peaceful ICT environment is essential for all and requires effective cooperation among States to reduce risks to international peace and security. The present report reflects the recommendations of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and builds upon the work of previous Groups (see A/65/201 and A/68/98). The Group examined relevant international concepts and possible cooperative measures pertinent to its mandate. It reaffirmed that it is in the interest of all States to promote the use of ICTs for peaceful purposes and to prevent conflict arising from their use.

# II. Existing and emerging threats

3. ICTs provide immense opportunities for social and economic development and continue to grow in importance for the international community. There are, however, disturbing trends in the global ICT environment, including a dramatic increase in incidents involving the malicious use of ICTs by State and non-State actors. These trends create risks for all States, and the misuse of ICTs may harm international peace and security.

4. A number of States are developing ICT capabilities for military purposes. The use of ICTs in future conflicts between States is becoming more likely.

5. The most harmful attacks using ICTs include those targeted against the critical infrastructure and associated information systems of a State. The risk of harmful ICT attacks against critical infrastructure is both real and serious.

6. The use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security.

7. The diversity of malicious non-State actors, including criminal groups and terrorists, their differing motives, the speed at which malicious ICT actions can occur and the difficulty of attributing the source of an ICT incident all increase risk. States are rightfully concerned about the danger of destabilizing misperceptions, the potential for conflict and the possibility of harm to their citizens, property and economy.

8. Different levels of capacity for ICT security among States can increase vulnerability in an interconnected world.

## III. Norms, rules and principles for the responsible behaviour of States

9. The ICT environment offers both opportunities and challenges to the international community in determining how norms, rules and principles can apply to State conduct of ICT-related activities. One objective is to identify further voluntary, non-binding norms for responsible State behaviour and to strengthen common understandings to increase stability and security in the global ICT environment.

10. Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability. Accordingly, norms do not seek to limit or prohibit action that is otherwise consistent with international law. Norms reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States. Norms can help to prevent conflict in the ICT environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development.

11. Previous reports of the Group reflected an emerging consensus on responsible State behaviour in the security and use of ICTs derived from existing international norms and commitments. The task before the present Group was to continue to study, with a view to promoting common understandings, norms of responsible State behaviour, determine where existing norms may be formulated for application to the ICT environment, encourage greater acceptance of norms and identify where additional norms that take into account the complexity and unique attributes of ICTs may need to be developed.

12. The Group noted the proposal of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan for an international code of conduct for information security (see A/69/723).

13. Taking into account existing and emerging threats, risks and vulnerabilities, and building upon the assessments and recommendations contained in the 2010 and 2013 reports of the previous Groups, the present Group offers the following recommendations for consideration by States for voluntary, non-binding norms, rules or principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment:

(a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;

(b) In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;

(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

(d) States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;

(e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;

(f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

(g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;

(h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;

(i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

(j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

(k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

14. The Group observed that, while such measures may be essential to promote an open, secure, stable, accessible and peaceful ICT environment, their implementation may not immediately be possible, in particular for developing countries, until they acquire adequate capacity.

15. Given the unique attributes of ICTs, additional norms could be developed over time.

## IV. Confidence-building measures

16. Confidence-building measures strengthen international peace and security. They can increase interstate cooperation, transparency, predictability and stability. In their work to build confidence to ensure a peaceful ICT environment, States should take into consideration the Guidelines for Confidence-building Measures adopted by the Disarmament Commission in 1988 and endorsed by consensus by the General Assembly in resolution 43/78 (H). To enhance trust and cooperation and reduce the risk of conflict, the Group recommends that States consider the following voluntary confidence-building measures:

(a) The identification of appropriate points of contact at the policy and technical levels to address serious ICT incidents and the creation of a directory of such contacts;

(b) The development of and support for mechanisms and processes for bilateral, regional, subregional and multilateral consultations, as appropriate, to enhance inter-State confidence-building and to reduce the risk of misperception, escalation and conflict that may stem from ICT incidents;

(c) Encouraging, on a voluntary basis, transparency at the bilateral, subregional, regional and multilateral levels, as appropriate, to increase confidence and inform future work. This could include the voluntary sharing of national views and information on various aspects of national and transnational threats to and in the use of ICTs; vulnerabilities and identified harmful hidden functions in ICT products; best practices for ICT security; confidence-building measures developed in regional and multilateral forums; and national organizations, strategies, policies and programmes relevant to ICT security;

(d) The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders. These measures could include:

(i) A repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of materials deemed appropriate for distribution on these national laws and policies;

(ii) The development of mechanisms and processes for bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure;

(iii) The development on a bilateral, subregional, regional and multilateral basis of technical, legal and diplomatic mechanisms to address ICT-related requests;

(iv) The adoption of voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents.

17. States should consider additional confidence-building measures that would strengthen cooperation on a bilateral, subregional, regional and multilateral basis. These could include voluntary agreements by States to:

(a) Strengthen cooperative mechanisms between relevant agencies to address ICT security incidents and develop additional technical, legal and diplomatic mechanisms to address ICT infrastructure-related requests, including the consideration of exchanges of personnel in areas such as incident response and law enforcement, as appropriate, and encouraging exchanges between research and academic institutions;

(b) Enhance cooperation, including the development of focal points for the exchange of information on malicious ICT use and the provision of assistance in investigations;

(c) Establish a national computer emergency response team and/or cybersecurity incident response team or officially designate an organization to fulfil this role. States may wish to consider such bodies within their definition of critical infrastructure. States should support and facilitate the functioning of and cooperation among such national response teams and other authorized bodies;

(d) Expand and support practices in computer emergency response team and cybersecurity incident response team cooperation, as appropriate, such as information exchange about vulnerabilities, attack patterns and best practices for mitigating attacks, including coordinating responses, organizing exercises, supporting the handling of ICT-related incidents and enhancing regional and sector-based cooperation;

(e) Cooperate, in a manner consistent with national and international law, with requests from other States in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory.

18. The Group reiterates that, given the pace of ICT development and the scope of the threat, there is a need to enhance common understandings and intensify cooperation. In this regard, the Group recommends regular institutional dialogue with broad participation under the auspices of the United Nations, as well as regular dialogue through bilateral, regional and multilateral forums and other international organizations.

## V. International cooperation and assistance in ICT security and capacity-building

19. States bear primary responsibility for national security and the safety of their citizens, including in the ICT environment, but some States may lack sufficient capacity to protect their ICT networks. A lack of capacity can make the citizens and critical infrastructure of a State vulnerable or make it an unwitting haven for malicious actors. International cooperation and assistance can play an essential role in enabling States to secure ICTs and ensure their peaceful use. Providing assistance to build capacity in the area of ICT security is also essential for international security, by improving the capacity of States for cooperation and collective action. The Group agreed that capacity-building measures should seek to promote the use of ICTs for peaceful purposes.

20. The Group endorsed the recommendations on capacity-building in the 2010 and 2013 reports. The 2010 report recommended that States identify measures to

support capacity-building in less developed countries. The 2013 report called upon the international community to work together in providing assistance to: improve the security of critical ICT infrastructure; develop technical skills and appropriate legislation, strategies and regulatory frameworks to fulfil their responsibilities; and bridge the divide in the security of ICTs and their use. The present Group also emphasized that capacity-building involves more than a transfer of knowledge and skills from developed to developing States, as all States can learn from each other about the threats that they face and effective responses to those threats.

21. Continuing the work begun through previous United Nations resolutions and reports, including General Assembly resolution 64/211, entitled "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures", States should consider the following voluntary measures to provide technical and other assistance to build capacity in securing ICTs in countries requiring and requesting assistance:

(a) Assist in strengthening cooperative mechanisms with national computer emergency response teams and other authorized bodies;

(b) Provide assistance and training to developing countries to improve security in the use of ICTs, including critical infrastructure, and exchange legal and administrative best practices;

(c) Assist in providing access to technologies deemed essential for ICT security;

(d) Create procedures for mutual assistance in responding to incidents and addressing short-term problems in securing networks, including procedures for expedited assistance;

(e) Facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders;

(f) Develop strategies for sustainability in ICT security capacity-building efforts;

(g) Prioritize ICT security awareness and capacity-building in national plans and budgets, and assign it appropriate weight in development and assistance planning. This could include ICT security awareness programmes designed to educate and inform institutions and individual citizens. Such programmes could be carried out in conjunction with efforts by international organizations, including the United Nations and its agencies, the private sector, academia and civil society organizations;

(h) Encourage further work in capacity-building, such as on forensics or on cooperative measures to address the criminal or terrorist use of ICTs.

22. The development of regional approaches to capacity-building would be beneficial, as they could take into account specific cultural, geographic, political, economic or social aspects and allow a tailored approach.

23. In the interest of ICT security capacity-building, States may consider forming bilateral and multilateral cooperation initiatives that would build on established partnership relations. Such initiatives would help to improve the environment for effective mutual assistance between States in their response to ICT incidents and could be further developed by competent international organizations, including the

United Nations and its agencies, the private sector, academia and civil society organizations.

## VI. How international law applies to the use of ICTs

24. The 2013 report stated that international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. Pursuant to its mandate, the present Group considered how international law applies to the use of ICTs by States.

25. The adherence by States to international law, in particular their Charter obligations, is an essential framework for their actions in their use of ICTs and to promote an open, secure, stable, accessible and peaceful ICT environment. These obligations are central to the examination of the application of international law to the use of ICTs by States.

26. In considering the application of international law to State use of ICTs, the Group identified as of central importance the commitments of States to the following principles of the Charter and other international law: sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States.

27. State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.

28. Building on the work of the previous Groups, and guided by the Charter and the mandate contained in General Assembly resolution 68/243, the present Group offers the following non-exhaustive views on how international law applies to the use of ICTs by States:

(a) States have jurisdiction over the ICT infrastructure located within their territory;

(b) In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States. Existing obligations under international law are applicable to State use of ICTs. States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms;

(c) Underscoring the aspirations of the international community to the peaceful use of ICTs for the common good of mankind, and recalling that the Charter applies in its entirety, the Group noted the inherent right of States to take measures consistent with international law and as recognized in the Charter. The Group recognized the need for further study on this matter;

(d) The Group notes the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction;

(e) States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts;

(f) States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. The Group noted that the accusations of organizing and implementing wrongful acts brought against States should be substantiated.

29. The Group noted that common understandings on how international law applies to State use of ICTs are important for promoting an open, secure, stable, accessible and peaceful ICT environment.

## VII. Conclusions and recommendations for future work

30. There has been significant progress in recognizing the risks to international peace and security from the malicious use of ICTs. Recognizing that ICTs can be a driving force in accelerating progress towards development, and consistent with the need to preserve global connectivity and the free and secure flow of information, the Group considered it useful to identify possible measures for future work, which include, but are not limited to, the following:

(a) Further development by States collectively and individually of concepts for international peace and security in the use of ICTs at the legal, technical and policy levels;

(b) Increased cooperation at regional and multilateral levels to foster common understandings on the potential risks to international peace and security posed by the malicious use of ICTs and on the security of ICT-enabled critical infrastructure.

31. While States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations.

32. Areas where further research and study could be useful include concepts relevant to State use of ICTs. The United Nations Institute for Disarmament Research, which serves all Member States, is one such entity that could be requested to undertake relevant studies, as could other relevant think tanks and research organizations.

33. The United Nations should play a leading role in promoting dialogue on the security of ICTs in their use by States and developing common understandings on the application of international law and norms, rules and principles for responsible State behaviour. Further work could consider initiatives for international dialogue and exchange on ICT security issues. These efforts should not duplicate ongoing

work by other international organizations and forums addressing issues such as criminal and terrorist use of ICTs, human rights and Internet governance.

34. The Group noted the importance of the consideration by the General Assembly of the convening of a new Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security in 2016 to continue to study, with a view to promoting common understandings on existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as how international law applies to the use of ICTs by States, including norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building.

35. The Group acknowledges the valuable efforts in ICT security made by international organizations and regional groups. Work among States on security in the use of ICTs should take these efforts into account, and Member States should, when appropriate, encourage the establishment of new bilateral, regional and multilateral platforms for dialogue, consultation and capacity-building.

36. The Group recommends that Member States give active consideration to the recommendations contained in the present report on how to help to build an open, secure, stable, accessible and peaceful ICT environment and assess how they might be taken up for further development and implementation.

## Annex

### List of members of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

**Belarus**
Aliaksandr Chasnouski (third and fourth sessions)
Deputy Head of the Department of International Security and Arms Control, Ministry of Foreign Affairs

Ambassador Vladimir N. Gerasimovich (first session)
Head of the Department of International Security and Arms Control, Ministry of Foreign Affairs

Ivan Grinevich (second session)
Counsellor at the Permanent Mission of Belarus to the United Nations in Geneva

**Brazil**
Carlos Luis Dantas Coutinho Perez
Minister, Chief of Staff of the Vice-Minister for Political Affairs, Ministry of External Relations

**China**
Haitao Wu (third and fourth sessions)
Coordinator for Cyber Affairs of Ministry of Foreign Affairs

Cong Fu (first and second sessions)
Coordinator for Cyber Affairs of Ministry of Foreign Affairs

**Colombia**
Jorge Fernando Bejarno
Director of Standards and Architecture of Information Technology, Ministry of Information Communications Technology

**Egypt**
Sameh Aboul-Enein
Ambassador, Deputy Assistant Foreign Minister for Disarmament, International Security and Peaceful Uses of Nuclear Energy, Ministry of Foreign Affairs

Amr Aljowaily (third session)
Minister, Permanent Mission of Egypt to the United Nations

**Estonia**
Marina Kaljurand
Undersecretary and Legal Adviser, Ministry of Foreign Affairs

**France**
Florence Mangin
Ambassador, Coordinator for Cyber Security, Ministry of Foreign Affairs

Leonard Rolland (first session)
Department of Strategic Affairs, Security and Disarmament, Ministry of Foreign Affairs

**Germany**
Karsten Geier
Head, Cyber Policy Coordination Staff, Federal Foreign Office

**Ghana**
Mark-Oliver Kevor
Member of the Board of Directors of the National Communications Authority

**Israel**
Iddo Moed
Cyber Security Coordinator, Ministry of Foreign Affairs

**Japan**
Takashi Okada (third and fourth sessions)
Ambassador in charge of United Nations Affairs and Ambassador in charge of Cyber Policy, Deputy Director General, Foreign Policy Bureau, Ministry of Foreign Affairs

Akira Kono (second session)
Ambassador in charge of United Nations Affairs and Ambassador in charge of Cyber Policy, Deputy Director General, Foreign Policy Bureau, Ministry of Foreign Affairs

Takao Imafuku (first session)
Senior Negotiator on International Security Affairs, Foreign Policy Bureau, Ministry of Foreign Affairs

**Kenya**
Katherine Getao
ICT Secretary, Ministry of Information, Communications and Technology

**Malaysia**
Nur Hayuna Abd Karim (fourth session)
Principal Assistant Secretary, Cyber and Space Security Division, National Security Council

Md Shah Nuri bin Md Zain (first, second and third sessions)
Undersecretary, Cyber and Space Security Division, National Security Council

**Mexico**
Edgar Zurita
Attaché to the United States of America and Canada, Mexican National Security Commission — Federal Police

**Pakistan**
Ausaf Ali (first, second and fourth sessions)
Director General, Technical Branch, Strategic Plans Division, Joint Staff Headquarters

Khalil Hashmi (third session)
Minister, Permanent Mission of Pakistan to the United Nations

**Republic of Korea**
Chul Lee (second and fourth sessions)
Director, International Security Division, Ministry of Foreign Affairs

Hyuncheol Jang (first and third sessions)
Counsellor, Embassy of the Republic of Korea to the Kingdom of Belgium and the European Union

**Russian Federation**
Andrey V. Krutskikh
Special Representative of the President of the Russian Federation for International Cooperation in Information Security, Ambassador-at-large

**Spain**
Ricardo Mor (fourth session)
Ambassador-at-large for Cybersecurity, Ministry of Foreign Affairs and Cooperation

Alicia Moral (first, second and third sessions)
Ambassador-at-large for Cybersecurity, Ministry of Foreign Affairs and Cooperation

**United Kingdom of Great Britain and Northern Ireland**
Olivia Preston
Assistant Director, Office of Cyber Security and Information Assurance, Cabinet Office

**United States of America**
Michele G. Markoff
Deputy Coordinator for Cyber Issues, Office of the Coordinator for Cyber Affairs, Office of the Secretary of State, United States Department of State